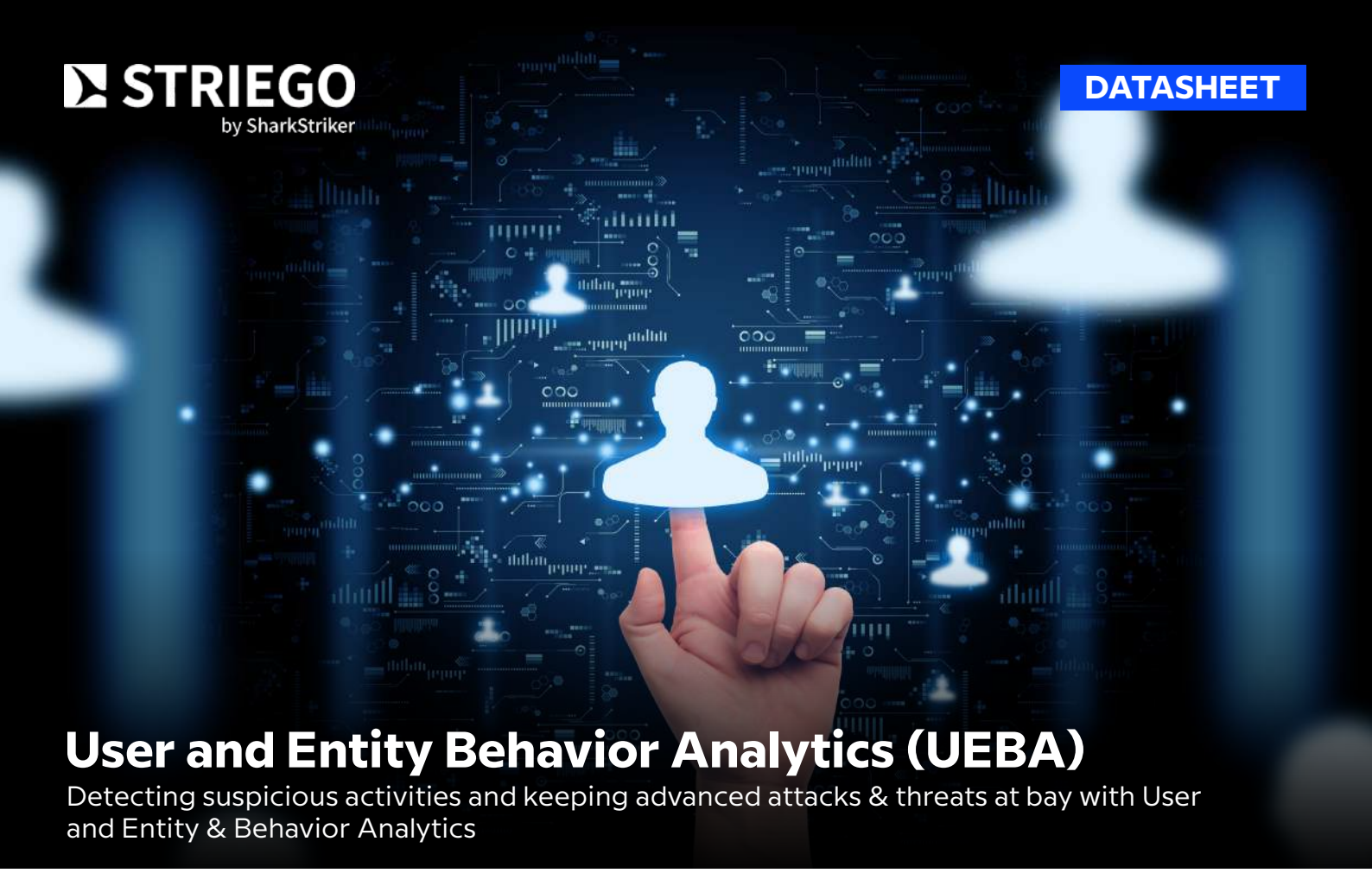
STRIEGO
by SharkStriker

DATASHEET



User and Entity Behavior Analytics (UEBA)

Detecting suspicious activities and keeping advanced attacks & threats at bay with User and Entity & Behavior Analytics

What is UEBA?

User and Entity Behavior Analytics is a security solution feature.
It detects suspicious and anomalous behavior across IT infrastructure. It uses AI and ML to detect, identify and prevent advanced internal network-based and other attacks on users or assets connected.

It continuously analyzes data from multiple sources like endpoints, identity, servers, and cloud. It derives a combined risk score to help experts to be more precise and efficient in their security operations. It is used along with SIEM/XDR to enhance its capability and to detect suspicious activities and catch perpetrators before they engage in advanced attacks. Our platform comes integrated with UEBA to help you gain max value from your security solution.

Challenges

The following are the challenges faced by traditional SIEM/XDR without an integrated UEBA :

- It gave a narrow view of the risk exposure in an organization.
- Traditional SIEM did not cover a wide range of attacks like Brute force attacks, DDoS attacks etc.
- Traditional SIEM gave limited context to security teams on user activities that were stealthy in nature like insider threats that were often hard to detect.
- SIEM/XDR focuses on detection based on IoCs and known patterns of attacks, whereas UEBA gives a contextual understanding through behavioral analysis, taking factors into consideration like role based access, location and time of activity.
- It takes more time for security analysts to analyze and make sense of alerts.

UEBA Benefits

The following are the ways through which the UEBA helps solve the above challenges:

Extensive Risk Visibility:
It offers a combined risk score from multiple sources such as endpoints, networks, identity, cloud, etc. It is based on critical assets marked by the user, file integrity monitoring, baseline security assessment, and vulnerability assessment.

User Activity Time line:
Provides a detailed summary of daily user activity along with the attack chain as per the time line with tags of notable events IOC detection etc.)

Combined Risk Evaluation:
It provides a combined risk score of detections, noteworthy events, and IoC and IoAs (Indicators of Compromise and Indicators of Attack)

STRIEGO - UEBA Unique Values Delivered

The following are the ways through which the UEBA helps solve the above challenges:

- Traditional UEBA may assess risk exposure based on alerts as per use cases. However, our UEBA calculates risk exposure based on alerts, events, and anomalies.
- A risk score based on 24-hour fluctuations and max score in 7 days as opposed to the average for more accuracy and to prevent overestimated risk score.
- Renders departmental assessment of risks.
- Determines the hacking tools used to detect malicious activity.
- It caters to the following use cases:
  - Checks for rare logins and unauthorized access
  - Detects suspicious activities like :
    - Lateral movements
    - Insider threats
    - Malware
    - Brute Force Attack
    - Credential dumping
    - Unauthenticated access - authentication against a new domain controller
    - Login attempts to server from different locations - tracks logins across multiple sources and locations connected to the network.
    - Data exfiltration attempts that cause data loss outside the network from one or different endpoints - continuous monitoring of the network for data loss.

What Are Some Of The Key Values (In Short)

- Offers a comprehensive risk score from multiple sources.
- Provides the complete time line of activities along with a complete attack chain.
- 24-hr Vulnerability Map with peak times.

How does it work?

About SharkStriker

SharkStriker is a trailblazing cybersecurity services vendor with a mission to simplify cybersecurity for its partners across industries through its technologically driven human-led open architecture platform STRIEGO. It seeks to cater to some of the industry's most immediate challenges such as siloed cybersecurity, increasing cost of cybersecurity solutions, changing regulatory environment, and increasing reliance on multiple vendors for multiple aspects of cybersecurity and compliance.

With STRIEGO, SharkStriker is able to assist its network of partners and customers through effective augmentation of cybersecurity posture as per use cases, extending visibility, compliance management, and round-the-clock support for incident response.

Through a team of threat-striking experts, they have made their presence across MEA, North America, Europe, and Asia.

Globally recognized, Globally trusted.

Phone: +1 925 5321900
Email: sales@sharkstriker.com
Website: www.sharkstriker.com

SharkStriker